UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/755,470	01/05/2001	Steven Branigan		4994

27997 7590 04/19/2006

PRIEST & GOLDSTEIN PLLC
5015 SOUTHPARK DRIVE
SUITE 230
DURHAM, NC 27713-7736

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/755,470	BRANIGAN ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: 6 February 2006 with original application filed on 05 January 2001 and acknowledgement of priority established by affidavit to 22 February 2000.

2. Claims 1-15 are currently pending in this application. Claims 1, 7, and 10 are independent claims.

Response to Arguments

3. Applicant's arguments with respect to claims 1-15 have been considered but are moot in view of the new ground(s) of rejection, which is necessitated by the affidavits submitted 6 February 2006.

Claim Objections

4. Claims 1-15 are objected to because of the following informalities: The heading on the claims submitted 1 September 2004, indicate that the claims are for application 09/533,396. Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

6. **Claims 1, 7, and 10** are rejected under 35 U.S.C. 102(e) as being anticipated by Ekberg U.S. Patent No. 7,003,282 (hereinafter '282).

As to independent claim 1, "A wired network for providing secure, authenticated access to wireless network clients, comprising:" is taught in '282 col. 2, lines 9-41;

"a server connected to a wireless network access point, and having access to the wired network, the server being operative to perform authentication for a wireless client establishing a connection to the server through the wireless network access point" is shown in '282 col. 3, line 60 through col. 4, line 29;

"the server performing authentication by examining authentication information transmitted from the client to the server and determining whether or not the authentication information identifies the wireless network client as authorized to gain access to the wired network" is disclosed in '282 col. 6 line 51 through col. 6, line 29;

"the server being operative to establish a connection session upon authentication of a client, the server being also operative to provide the client with a wired network address valid for the connection session upon authentication of the client" is taught in '282 col. 4, line 63 through col. 5, line 50;

"the server being further operative to encrypt communications with the wireless network access point" is shown in '282 col. 4, lines 45-56;

"the server being further operative to provide a cryptographic key valid for the connection session to the client upon authentication of the client; and a user database accessible to the server for use in validating wireless clients" is disclosed in '282 col. 6, lines 40-65.

As to independent 7, "A wireless network for providing secure authenticated communication between clients of the wireless network and a wired network, comprising:" is taught in '282 col. 2, lines 9-41;

"a wireless network access point operative to establish a connection with a server operating as a portal between the wireless network and a wired network the wireless network access point being operative to conduct communications with the server in order to authenticate wireless network clients as authorized to access the wired network" is shown in '282 col. 3, line 60 through col. 4, line 29;

"the wireless network access point being further operative to receive authentication information from one or more wireless network clients and transfer the authentication information to the server in order to allow the server to examine the authentication information for a wireless network client and determine if the information indicates that the wireless network client is authorized to access the wired network" is disclosed in '282 col. 6 line 51 through col. 6, line 29;

"the wireless network access point being operative to receive a cryptoprocessing key from the server upon authentication of a client and to transfer the key to that client" is taught in '282 col. 6, lines 40-65;

"and a plurality of wireless network clients operative to establish connections with the wireless network access point" is shown in '282 col. 7, line 44 through col. 8, line 16 (note '282 is interpreted to serve several clients);

"each client being operative to conduct encrypted communications with the server through the access point" is disclosed in '282 col. 4, lines 45-50;

"to pass authentication information to the network access point in order to indicate to a server communicating with the wireless network and a wired network" is taught in '282 col. 4, line 53 through col. 5, line 50;

"whether or not the wireless client is authorized to gain access to the wired network, each wireless network client being further operative to and receive address information and crypto-processing data from the network access point upon authentication by the server in order to allow communication with the wired network" is shown in '282 col. 5, line 51 through col. 6, line 20;

"each client being operative to conduct encrypted transfer of data to and from the wired network through the access point upon receiving the address and cryptoprocessing information" is shown in '282 col. 4, lines 45-56.

As to independent 10, "A method of secure communication between wireless network clients and a wired network, comprising the steps of:" is taught in '282 col. 2, lines 9-41;

"establishing a connection between a wireless network access point and a security base (SB) server connected to the wired network; establishing a connection between the SB server and a wireless network client communicating with the SB server through the wireless network access point" is shown in '282 col. 3, line 60 through col. 4, line 29;

"exchanging encryption keys between the SB server and the wireless network client" " is disclosed in '282 col. 6, lines 40-65;

"transmitting authentication information from the wireless network client to the SB server through the wireless network access point; performing authentication for the

wireless network client by examining the authentication information to determine if the wireless network client is authorized to gain access to the wired network" is taught in '282 col. 6 line 51 through col. 6, line 29;

"if authentication fails, rejecting connection to the wired network" is shown in '282 col. 6, lines 53-65 (note the authentication done by the GSM network as well as the challenges stored in the database will reject connection to the wired network if authentication fails, i.e. "no reply will be given to the challenge" line 60);

"and if authentication passes, accepting connection to the wired network, providing a temporary wired network address" is taught in '282 col. 4, line 63 through col. 5, line 50;

"and a unique session encryption key to the wireless network client" is disclosed in '282 col. 6, lines 40-65;

"and providing access to wired network resources in response to requests by the wireless network client" is shown in '282 col. 10, lines 4-43.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 2, 3, 8, and 9,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '282 as applied to claims 1 and 7 in further view of Feder et al. U.S. Patent Publication No. 2002/0089958 hereinafter '958).

As to dependent claim 2, the following is not taught in '282: **"also including a network hub providing connections between the server and additional resources on the wired network"** however '958 teaches "It is an object of the present system to provide a wireless packet switched data network for end users that divides mobility management into local, micro, macro and global connection handover categories and minimizes handoff updates according to the handover category ... It is yet another object to provide an intermediate XTunnel channel between a wireless hub (also called access hub AH) and an inter-working function unit (IWF unit) in a foreign network. It is yet another object to provide an IXTunnel channel between an inter-working function unit in a foreign network and an inter-working function unit in a home network. It is yet another object to enhance the layer two tunneling protocol (L2TP) to support a mobile end system. It is yet another object to perform network layer registration before the start of a PPP communication session" on page 1, paragraph 0012.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access as well as an authentication/negotiation component with service providers taught in '282 to include a means to provide access to private network services and resources. One of ordinary skill in the art would have been motivated to perform such a modification to increase the level of wireless services available to a customer see '958 (page 1, paragraph 0010). "Today, internet service providers offer internet access services, web content services, e-mail services, content hosting services and roaming to end users. Because of low margins and no scope of doing market segmentation based on features and price, ISPs are looking for value added services to improve margins. In the short term, equipment vendors will be able to offer solutions to ISPs to enable them to offer faster

access, virtual private networking (which is the ability to use public networks securely as private networks and to connect to intranets), roaming consortiums, push technologies and quality of service ... Wireless service providers will be able to capture a larger share of the revenue stream. The ISP will be able to offer more services and with better market segmentation".

As to dependent 3, "also including a router providing connections between the server and additional resources on the wired network as well as a connection to an additional wired network" is disclosed in '958 page 1, paragraph 0012.

As to dependent 8, "wherein the access point communicates with the server using point to point tunneling protocol" is shown in '958 pages 3-4, paragraph 0056.

As to dependent 9, "including a hub connecting the wireless network access point and a plurality of additional network access points, each additional network access point communicating with a plurality of additional wireless network clients, the wireless network access point and- the additional network access points being operative to establish connections with the server through the network hub" is disclosed in '958 on page 1, paragraph 0012.

9. **Claims 4-6,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '282 in further view '958 in further view of Massarani U.S. Patent No. 6,393,484 (hereinafter '484).

As to dependent 4, the following is not taught in the combination of '282 and '958 **"wherein the server is operative to provide addresses to clients through dynamic host control protocol"** however '484 teaches "These and other objects, features and advantages are achieved in a system comprising communication layers (OSI 2 and 3) and work equipment

(routers and/or switches) which work in conjunction with Dynamic Host Control Protocols (DHCP) and Address Resolution Protocols (ARP)" in col. 3, lines 19-44.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access as well as an authentication/negotiation component with service providers taught in the combination of '282 and '958 to include a means to utilized a dynamic host control protocol. One of ordinary skill in the art would have been motivated to perform such a modification to prevent unauthorized visitors see '484 (col. 1, lines 14 et seq.). "With the vast increase of private, semi-public and public shared-medium IP networks, a growing problem for network and service administrators is how to control and restrict access to the networks only to authorized and registered devices and users. One example of the problem relates to corporate IP network administrators who deal with an increasingly mobile work force that have deployed IP network access ports (typically IEEE 802.X or similar medium) throughout their corporate facilities for shared use by their corporate employees. Such shared network access ports work in conjunction with Dynamic Host Control Protocol (DHCP) servers to dynamically assign the appropriate IP address and other parameters to a mobile employee's device. A strong concern in the use of such networks is preventing visitors or unauthorized persons from taking advantage of the exposed network access ports to gain IP connectivity to the internal corporate network (intranet)".

As to dependent 5, "wherein the server is operative to communicate with a wireless network client using point to point tunneling protocol" is shown in '958 pages 3-4, paragraph 0056 "The network infrastructure provides PPP (point-to-point protocol) service to end systems. The network provides (1) fixed wireless access with roaming (log-in anywhere that

the wireless coverage is available) to end systems and (2) low speed mobility and hand-offs. When an end system logs on to a network, in it may request either fixed service (i.e., stationary and not requiring handoff services) or mobile service (i.e., needing handoff services). An end system that does not specify fixed or mobile is regarded as specifying mobile service. The actual registration of the end system is the result of a negotiation with a home registration server based on requested level of service, the level of services subscribed to by the user of the end system and the facilities available in the network".

As to dependent 6, "wherein the server employs 128-bit crypto-processing to communicate with the wireless network client" is disclosed in '958 page 13, paragraph 0190 "End system authentication uses a 128-bit shared secret to create an authenticator for its registration request. The authenticator is created using the known MD5 message digest algorithm as described in the mobile IP RFC 2002. Alternatively, a different algorithm may be used".

10. **Claims 11 and 12,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '282 in view of Massarani U.S. Patent No. 6,393,484 (hereinafter '484).

As to dependent claim 11, "and wherein the step of accepting the connection is accompanied by a step of logging the acceptance" is taught in '282 col. 2, line 58 through col. 3, line 4 "With the solution according to the invention such an advantage is also achieved in connection with fixed terminals, that functions built in connection with the mobile communications network can be utilized in connection with Internet services. E.g. an organization working both as a mobile communication operator and as an ISP operator may use charging services built in connection with the mobile communications network for charging for the Internet services which he provides. When also fixed terminals are authenticated with the

method according to the invention, much certainty is achieved that the bill will be directed at the correct subscriber. In addition, the subscriber can be authenticated, even if he attaches to the network from a foreign terminal";

the following is not taught in '341 **"wherein the step of rejecting connection to the wired network is accompanied by a step of logging the rejection"** however '484 teaches "If the MAC address is not registered, the DHCP server refuses to handle the request, logs the attempt, potentially alerting network operators of a security breach" in col. 3, lines 33-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access as well as an authentication/negotiation component with service providers taught in '282 to include a means to log rejections. One of ordinary skill in the art would have been motivated to perform such a modification to prevent unauthorized visitors see '484 (col. 1, lines 14 et seq.). "With the vast increase of private, semi-public and public shared-medium IP networks, a growing problem for network and service administrators is how to control and restrict access to the networks only to authorized and registered devices and users. One example of the problem relates to corporate IP network administrators who deal with an increasingly mobile work force that have deployed IP network access ports (typically IEEE 802.X or similar medium) throughout their corporate facilities for shared use by their corporate employees. Such shared network access ports work in conjunction with Dynamic Host Control Protocol (DHCP) servers to dynamically assign the appropriate IP address and other parameters to a mobile employee's device. A strong concern in the use of such networks is preventing visitors or unauthorized persons from taking advantage of

the exposed network access ports to gain IP connectivity to the internal corporate network (intranet)".

As to dependent 12, "wherein the step of providing a temporary wired network address to the wireless network client includes using dynamic host control protocol to provide the address" is shown in '484 col. 3, lines 19-44.

11. **Claim 13** is rejected under 35 U.S.C. 103(a) as being unpatentable over '282 in view of '484 in further view of Feder et al. U.S. Patent Publication No. 2002/0089958 hereinafter '958).

As to dependent 13, the following is not taught in the combination of '282 and '484: **"wherein communication between the wireless network client and the wired network server is performed using point to point tunneling protocol"** however '958 teaches "The network infrastructure provides PPP (point-to-point protocol) service to end systems. The network provides (1) fixed wireless access with roaming (log-in anywhere that the wireless coverage is available) to end systems and (2) low speed mobility and hand-offs. When an end system logs on to a network, in it may request either fixed service (i.e., stationary and not requiring handoff services) or mobile service (i.e., needing handoff services). An end system that does not specify fixed or mobile is regarded as specifying mobile service. The actual registration of the end system is the result of a negotiation with a home registration server based on requested level of service, the level of services subscribed to by the user of the end system and the facilities available in the network" on pages 3-4, paragraph 0056.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access as well as an authentication/negotiation component with service providers taught in the combination of '282

and '484 to include a means to provide access to private network services and resources. One of ordinary skill in the art would have been motivated to perform such a modification to increase the level of wireless services available to a customer see '958 (page 1, paragraph 0010). "Today, internet service providers offer internet access services, web content services, e-mail services, content hosting services and roaming to end users. Because of low margins and no scope of doing market segmentation based on features and price, ISPs are looking for value added services to improve margins. In the short term, equipment vendors will be able to offer solutions to ISPs to enable them to offer faster access, virtual private networking (which is the ability to use public networks securely as private networks and to connect to intranets), roaming consortiums, push technologies and quality of service ... Wireless service providers will be able to capture a larger share of the revenue stream. The ISP will be able to offer more services and with better market segmentation".

12. **Claims 14-15** are rejected under 35 U.S.C. 103(a) as being unpatentable over '282 in further view of '484 in further view of '958 in further view of Schuster et al. U.S. Patent No. 6,857,072 (hereinafter '072).

As to dependent 14, "wherein the step of performing authentication for the wireless network client includes transferring authentication information between the wireless network client and the SB server and wherein the authentication information is encrypted" is taught in '282 col. 4, lines 45-56;

the following is not taught in the '282, '484, and '958 combination:

"using public key cryptography" however '072 teaches "One advantage of the PID-Enabled Data Network Telephony System 100 in FIG. 1 is that it may be used to provide

encryption and/or authentication services. In one embodiment, the PID 110 is able to determine and exchange encryption and/or authentication data, such as a public encryption and/or authentication keys ... over a privacy network" in col. 6, lines 44-64.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access as well as an authentication/negotiation component with service providers that also tracks rejections taught in the combination of '341 and '484 to include a means to utilize a public/private key encryption mechanism. One of ordinary skill in the art would have been motivated to perform such a modification so that sensitive data may be transmitted more securely see '072 (col. 3, lines 30 et seq.). "The present invention addresses the above needs by providing a system in a data network telephony system, such as for example, the Internet, that enables encryption and/or authentication on the telephony system. Users may participate in transactions with each other using more secure data channels. Sensitive data may be transmitted more safely across public networks"

As to dependent 15, "wherein the step of providing a unique session encryption key includes encrypting the unique session encryption key" is taught in ''282 col. 6, lines 40-65;

"using public key cryptography" is shown in '072 col. 6, lines 44-64.

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
08 April 2006